Operations Security in an Age of Radical Transparency

By Dennis M. Murphy

We often hearken back to the Cold War as a simpler time… not because of the danger it portended, but because of the nature of the threat. That bipolar world defined a clear enemy with an order of battle that could be templated and processes and methodologies that could be studied. It was a two dimensional world of good and bad. Operations security (OPSEC), defined as "select(ing) and execut(ing) measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation," was equally cut and dry. But, oh how the world has changed. Not only is the adversary often an amorphous entity, he also both understands and exploits a new environment that empowers him with information as an asymmetric weapon of choice. Those factors certainly complicate the military operating environment of today, but the waters are muddied further when non-combatants can willingly, or unwittingly, impact operations through ready access to real-time media means. Further complicating matters is a generation of soldiers, sailors, airmen and Marines who expect to use new media to communicate freely, at the click of a mouse, to a potentially global audience. The result is a situation that significantly increases the complexity of OPSEC, demanding commanders' emphasis to mitigate risk and protect friendly operations while still allowing the ability to effectively fight and win the war of ideas. The answer lies by focusing on OPSEC within the current military planning process and increased attention to educating soldiers to enhance and protect military operations.

The Information Environment: A Two Edged Sword

The current information environment has leveled the playing field for not only nation states, but non-state actors, multinational corporations and even individuals to affect strategic outcomes with minimal information infrastructure and little capital expenditure. Even a cursory look at advances in technology confirms what most people recognize as a result of their daily routine. The ability to access, collect, and transmit information is clearly decentralized to the lowest level (the individual). Anyone with a camera cell phone and personal digital device with Internet capability understands this. The technology is increasingly smaller, faster and cheaper. Consequently, the ability to control and verify information is much more limited than in the recent past. Nor will it get any easier.

And, while Internet penetration in some of the most contentious parts of the world is certainly limited, it is growing exponentially. Africa has only a 4.7% Internet penetration based on population, but the use of the Internet grew 883% there from 2000 to 2007. Dramatic growth rates are similarly occurring in Asia, the Middle East and Latin America. Technological advances such as the use of television "white space" for wireless Internet usage and the $100 laptop project provide just a sampling of innovation that will place the World Wide Web in the hands of the underdeveloped world; the same world where future United States conflicts might occur. This is not to ignore the impact of cell phone telephony. The cell phone as a means of mobile technology, is increasingly available worldwide and deserves discussion as a potentially potent capability to affect national security and military issues; arguably even more so than the Internet. So, increasingly, anyone in the world can become an "iReporter" uploading their photos and stories to the Web with the ability to reach a worldwide audience.

This same explosion of information technology that has enabled individuals around the world is certainly embraced and exploited by junior soldiers, sailors, airmen and Marines. The Pew Internet and American Life Project shows a dramatic increase in the number of U.S. adults online beginning in 1995. Considering the age of most enlistees and junior officers, it seems safe to say that they have grown up with the Internet as an integral part of their lives. Consequently, soldiers expect to use new media to communicate today. This includes the use of social networking sites such as *MySpace* and *Facebook* among others, as well as active participation in Web logs (blogs). This same propensity to see the use of information technology as an immutable given of daily human intercourse has had interesting second order effects. Anecdotal evidence seems to indicate that many young people have lost the distinction between the public and private domains, posting entries to new media sites that result in both personal and professional scrutiny and dilemmas.

Access to immediate information in the hands of the many, along with a cultural attitude by military members regarding its use, presents new and important challenges to the warfighting commander. In this era of radical transparency, where absolute control may be impossible, military leaders must effectively—and actively—manage OPSEC.

OPSEC and Strategic Communication: Mitigating Risk while Exploiting Information

In the past OPSEC involved controlling soldiers; today it applies to anyone with access to new media in the military operating environment. Contractors, Non-Governmental Organizations (NGOs), and the local indigenous population (among others) with cell phones can report real time information on military operations immediately to any number of sources. While this is readily evident in counterinsurgency operations, it is increasing relevant across the spectrum of military operations given the proliferation of new media means. Therefore, it is essential to consider OPSEC in the military planning process in order to mitigate the risk posed by the

ubiquity of new media. Risk assessment is an integral part of joint planning. It begins during mission analysis and continues through course of action development, wargaming, and course of action comparison and selection, where risk mitigation is specifically considered. Given the significant risks posed by non-combatants with Internet or cell phone capability the chances of real time public release of friendly actions and vulnerabilities are considerable and easily subject to enemy exploitation. Consequently, risk and actions to mitigate it must be considered throughout the planning process with an increasing and special emphasis on OPSEC.

Savvy commanders, aware of the challenges posed by the information environment may choose to mitigate the OPSEC risk through the use of tactical deception, but this comes with potentially significant second and third order effects to other warfighting capabilities.

DOD defines strategic communication as:

Focused United States Government processes and efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable to advance national interests and objectives through the use of coordinated information, themes, plans, programs, and actions synchronized with other element of national power.

Parsing the definition to its essential parts, strategic communication is the integration of actions, images and words to send a message in order to affect perceptions, attitudes and ultimately behaviors. So, while deception can certainly aid in the security of an operation, it can also negate the credibility of any future messages the command wishes to send in an effort to persuade or influence the indigenous population in particular. The strategic communication effort is about trust and credibility and is critical to swaying a "fence sitting" population to friendly presence, especially in a counterinsurgency.

Maintaining OPSEC within the purview of the military unit would seemingly be an easier task, perhaps no different than in the past. But, once again, it should be viewed with an eye toward the impact on strategic communication. Blogs and social networking sites provide a forum to tell the military's story, often by the most credible sources: the soldiers, sailors, airmen or Marines themselves. These first hand stories become extremely important in today's information environment as a means to counter and provide an alternative to the negative reporting often found in the mainstream media. But risk aversion with an eye toward OPSEC often stymies the effort. Past military policies in Iraq have been restrictive and often discouraged blogging rather than encouraging it. In May 2008, Army Lieutenant Matthew Gallagher's blog "Kaboom" was taken down by his leadership after he recounted an anonymous exchange between himself and his commander without first seeking approval prior to posting. The site had received tens of thousands of page views about the day-to-day life of an Army platoon in the war zone prior to its demise. *MySpace* and *Facebook*, as previously noted, receive plenty of press about their transparency and the adverse effect of personal disclosure in the wrong hands. And so both blogs and social networks present operations security issues for commanders, rightly concerned about maintaining the secrecy of military operations, capabilities and vulnerabilities. A risk mitigation process must be established then, that can allow soldiers to tell the good news stories, while protecting OPSEC. Army Lieutenant General Bill Caldwell (interestingly using a blog as his medium of choice) offers some advice in this regard. He proffers that commanders should encourage soldiers to tell their stories; empower them by underwriting honest mistakes, specifically noting that leaders need to assume risk here; educate them on potential strategic implications of engagement (to include OPSEC) and; equip them to engage the new media.

Conclusion

The rapid evolution of the information environment ensures that future military operations will be increasingly complex. Our adversaries have shown both a significant ability and propensity to exploit information using new media means as an asymmetric weapon of choice. Additionally, non-combatants wield information as power as cell phone and Internet access proliferate. The U.S. military must fight back against this. But there are both challenges and opportunities in doing so. First, the commander, no longer in complete control of OPSEC, must place increasing emphasis on risk mitigation within the military planning process to protect against the release of friendly actions and vulnerabilities, and he must do so considering the second order effects on strategic communication. Second, as he has always done in the past, he must educate his soldiers, now specifically about the OPSEC considerations of new media, while empowering them to fight the war of ideas. This balance of risk mitigation to both protect OPSEC while leveraging information is essential to exploiting success in the current and future military operating environment.